RESTORATION OF A COMPUTER TO A PREVIOUS STATE

Publication number: JP2003503793T

Publication date: 2003-01-28

Inventor:

Applicant:

Classification:

- international: ***G06F11/14;*** **G06F11/14;** (IPC1-7): G06F9/445; G06F12/00

- european: G06F11/14A4B1M2; G06F11/14A4B1M10; G06F11/14A4C

Application number: JP20010507196T 20000630

Priority number(s): US19990141757P 19990630; WO2000US18324 20000630

Also published as:

WO0101285 (A3
WO0101285 (A2
WO0101255 (A1
WO0101255 (A1
WO0101252 (A1

more >>

Abstract not available for JP2003503793T
Abstract of corresponding document: **WO0101251**

Methods and systems for backing up and restoring the state of a computer system are disclosed. Computer resource use is minimized by combining the backup methods of file copying and file logging. During backup, copies are stored of those files that are expected to change frequently. For other files, changes are noted in a change log and backup copies may be made if they would be useful when later restoring the files. Restoration proceeds by overwriting the frequently-changing files with stored copies and by undoing the changes to the logged files.

(19)日本国特許庁（ＪＰ）　(12) **公表特許公報（Ａ）**　(11)特許出願公表番号
特表2003－503793
（P2003－503793A）
(43)公表日　平成15年１月28日(2003.1.28)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード(参考)
Ｇ０６Ｆ　9/445		Ｇ０６Ｆ　12/00	５３１Ｒ　５Ｂ０７６
12/00	５３１	9/06	６１０Ｌ　５Ｂ０８２

審査請求　未請求　予備審査請求　有　（全 28 頁）

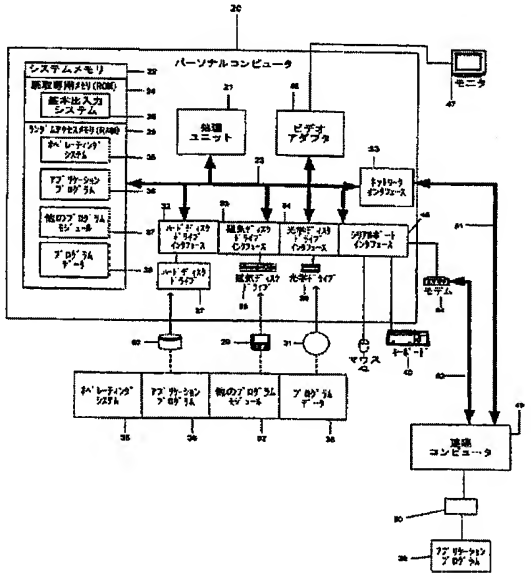
(21)出願番号　特願2001－507196(P2001－507196)
(86)（22)出願日　平成12年６月30日(2000.6.30)
(85)翻訳文提出日　平成13年12月28日(2001.12.28)
(86)国際出願番号　ＰＣＴ／ＵＳ００／１８３２４
(87)国際公開番号　ＷＯ０１／００１２５２
(87)国際公開日　平成13年１月４日(2001.1.4)
(31)優先権主張番号　６０／１４１，７５７
(32)優先日　平成11年６月30日(1999.6.30)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　マイクロソフト　コーポレイション
ＭＩＣＲＯＳＯＦＴ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国　ワシントン州　98052－6399　レッドモンド　ワン　マイクロソフト　ウェイ　（番地なし）
(72)発明者　シッカ　アシシュ
アメリカ合衆国　ワシントン州　98007　ベルヴュー　ワンハンドレッドアンドフォーティーエイス　アヴェニュー　ノースイースト　＃エム203　4385
(74)代理人　弁理士　中村　稔　（外９名）

最終頁に続く

(54)【発明の名称】　共用システムファイルを保護するシステム及び方法

(57)【要約】
共用システムファイルを保護するシステム及び方法は、アプリケーションにより共用されるＤＬＬファイルなどのシステムファイルがアプリケーションのインストール又は更新の間やユーザの行為によって無効なファイルで重ね書きされることを防ぐことによりシステムの安定性を高める。モニタリング構成要素は、システムファイルに対する変更を監視する。保護されたシステムファイルが変更されているのをモニタリング構成要素が検知した時、モニタリング構成要素は、オリジナルファイルのコピーを保存し、その変更をファイル保護サービスに報告する。ファイル保護サービスは、変更されたファイルを検査し、それが有効か否かを判断する。変更ファイルが無効である場合、システムファイルは、モニタリング構成要素が保存したコピーを用いてオリジナルの内容へ復元される。アプリケーション・インストーラ又は更新パッケージによるシステムファイルの未許可の持ち込みは、適切な権限を有する関係者が発行する証明書の使用を必要とすることにより防止される。



【特許請求の範囲】

【請求項１】　システムファイルに変更を行う呼び出しを監視する段階と、

保護されるべき共用システムファイルに対して行なわれている変更を検知する段階と、

前記共用システムファイルに前記変更が為される前に、前記共用システムファイルのコピーを保存する段階と、

前記共用システムファイルに対する前記変更が有効であるか否かを判断する段階と、

前記変更が無効である場合、前記共用システムファイルの前記保存されたコピーを用いて前記変更を取り消す段階と、

を含むことを特徴とする、コンピュータシステムの共用システムファイルを保護する方法。

【請求項２】　請求項１に記載の方法を実行するコンピュータ実行可能命令を有することを特徴とする、コンピュータ読出可能媒体。

【請求項３】　前記共用システムファイルに対して為される前記変更は、前記共用システムファイルの異なるバージョンによる重ね書きであることを特徴とする請求項１に記載の方法。

【請求項４】　前記判断段階は、前記共用システムファイルの前記異なるバージョンのバージョン番号を前記コンピュータシステムにインストールされた前記共用システムファイルの最高バージョンと比較する段階を含むことを特徴とする請求項３に記載の方法。

【請求項５】　前記比較段階は、前記コンピュータシステムにインストールされた保護システムファイルを識別するデータを包含するデータベースから、前記共用システムファイルの前記最高バージョンに関するデータを検索する段階を含むことを特徴とする請求項４に記載の方法。

【請求項６】　前記判断段階は、前記異なるバージョンのハッシュ値を前記コンピュータシステムにインストールされた前記最高バージョンのハッシュ値と比較する段階を更に含むことを特徴とする請求項５に記載の方法。

【請求項７】　前記ハッシュ値の比較段階は、前記共用システムファイルに

関するインストレーションカタログの識別子を前記データベースから検索する段階と、前記コンピュータシステムにインストールされた前記最高バージョンの前記ハッシュ値を得るために前記インストレーションカタログにアクセスする段階とを含むことを特徴とする請求項６に記載の方法。

【請求項８】　請求項７に記載の方法を実行するコンピュータ実行可能命令を有することを特徴とする、コンピュータ読出可能媒体。

【請求項９】　前記取り消し段階は、前記異なるバージョンを前記共用システムファイルの前記保存コピーで重ね書きする段階を含むことを特徴とする請求項３に記載の方法。

【請求項１０】　前記取り消し段階は、前記異なるバージョンを前記共用システムファイルの前記保存コピーで重ね書きするために、命令をシステム起動ファイルに挿入する段階を含むことを特徴とする請求項３に記載の方法。

【請求項１１】　前記共用コンピュータファイルは、ダイナミック・リンク・ライブラリ（ＤＬＬ）ファイルであることを特徴とする請求項１に記載の方法。

【請求項１２】　前記検知段階は、変更されている前記共用システムファイルが保護されるべきか否かを判断するために、保護システムファイルのリストを参照する段階を含むことを特徴とする請求項１に記載の方法。

【請求項１３】　更新パッケージを受け取る段階と、

前記更新パッケージの証明書を認証する段階と、

前記更新パッケージに含まれた共用システムファイルの更新バージョンを取り出す段階と、

前記コンピュータシステム上の前記共用システムファイルの現存バージョンを前記更新バージョンで重ね書きする段階と、

前記共用システムファイルの前記更新バージョンを含むために、前記コンピュータシステム上にインストールされた保護システムファイルを識別するデータベースを更新する段階と、

を更に含むことを特徴とする請求項１に記載の方法。

【請求項１４】　請求項１３に記載の方法を実行するコンピュータ実行可能

命令を有することを特徴とする、コンピュータ読出可能媒体。

【請求項１５】　コンピュータシステムの共用システムファイルを保護するコンピュータ実行可能な構成要素であって、

モニタリング構成要素と、

ファイル保護サービス構成要素と、

を含み、

前記モニタリング構成要素は、システムファイルに対する変更を監視し、保護共用システムファイルに対して為されている変更を検知すると前記変更が為される前に前記保護共用システムファイルのコピーを保存し、前記ファイル保護サービス構成要素に通知し、前記サービス構成要素は、前記通知に応答して前記変更が有効か否かを判断し、前記変更が有効でない場合には前記保護共用システムファイルの前記保存コピーを用いて前記変更を取り消す、

ことを特徴とする構成要素を有するコンピュータ読出可能媒体。

【請求項１６】　前記モニタリング構成要素は、システムファイルを変更するためのファイルシステムドライバへの呼出しを監視するために前記ファイルシステムドライバの上に置かれることを特徴とする請求項１５に記載のコンピュータ読出可能媒体。

【請求項１７】　前記共用システムファイルに対する前記変更は、前記共用システムファイルの異なるバージョンによる重ね書きであることを特徴とする請求項１５に記載のコンピュータ読出可能媒体。

【請求項１８】　前記ファイル保護サービス構成要素は、前記コンピュータシステム上にインストールされた保護システムファイルを識別するインストールされたファイルのデータベースを保持し、前記共用システムファイルの前記異なるバージョンが有効か否かを判断する際に前記インストールファイル・データベースを参照することを特徴とする請求項１５に記載のコンピュータ読出可能媒体。

【請求項１９】　前記インストールファイル・データベースは、前記コンピュータシステム上にインストールされた前記保護システムファイルの各々に対するインストールされた最高バージョンとハッシュ値とを識別し、前記ファイル保

護サービス構成要素は、変更されている前記保護システムファイルの前記インストールされた最高バージョンとハッシュ値とを前記異なるバージョンが有効か否かを判断するために使用することを特徴とする請求項１８に記載のコンピュータ読出可能媒体。

【請求項２０】　前記ファイル保護サービス構成要素は、保護ファイルリストを更に保持し、前記モニタリング構成要素は、前記変更が前記保護共用システムファイルに対して為されているのを検知すると前記保護ファイルリストにある前記保護共用システムファイルを識別することを特徴とする請求項１９に記載のコンピュータ読出可能媒体。

【請求項２１】　前記ファイル保護サービス構成要素は、

更新パッケージを受け取る段階と、

前記更新パッケージを認証する段階と、

前記更新パッケージに含まれた共用システムファイルの更新バージョンを取り出す段階と、

前記コンピュータシステム上の前記共用システムファイルの現存バージョンを前記更新バージョンで重ね書きする段階と、

前記共用システムファイルの前記更新バージョンを含むために、前記インストールファイル・データベースを更新する段階と、

を実行するように更にプログラムされることを特徴とする請求項２０に記載のコンピュータ読出可能媒体。

【請求項２２】　前記保護共用システムファイルは、ダイナミック・リンク・ライブラリ（ＤＬＬ）ファイルであることを特徴とする請求項１５に記載のコンピュータ読出可能媒体。

【発明の詳細な説明】

【０００１】

（技術分野）

本発明は、一般的にコンピュータオペレーティングシステムに関し、更に特定すれば、異なるアプリケーションが共用する重要なオペレーティングシステムファイルの保護に関する。

【０００２】

（背景技術）

今日のコンピュータオペレーティングシステムは、その構成に多くの層を有する場合があり、異なる機能を果たすために無数のファイルを含んだ高度に複雑なプログラムである。オペレーティングシステム（オペレーティングシステム）の構成要素の幾つかは、システムにインストールされたアプリケーションに様々なシステム機能を準備するように設計されており、従って、アプリケーションによって「共用」される。例えば、マイクロソフト・コーポレーションのＷＩＮＤＯＷＳ（登録商標）オペレーティングシステムには、アプリケーションプログラムが実行時にリンクしてそこに実装された機能を呼び出すことができる多くのファイルがダイナミック・リンク・ライブラリ（ＤＬＬ）ファイルの形で存在する。

【０００３】

ＤＬＬファイルなどの共用オペレーティングシステムファイルは、多数の異なるアプリケーションによって使用されるから、それらの共用システムファイルのうちの１つが変造されたり、不用意に重ね書きされたり、又は、他の方法で破壊されると、多くの数のアプリケーションが働きを停止する場合がある。従って、共用システムファイルに対する無効な変更は、システム不安定の重大な原因となる可能性がある。例えば、ＷＩＮＤＯＷＳ（登録商標）オペレーティングシステムは、第三者のアプリケーションのインストーラプログラムがこのアプリケーションによって必要とされる全てのファイルをこのアプリケーションのインストレーション中にシステムに加えることを許している。インストレーション中に加えられたそれらのファイルは、他のアプリケーションにより共用されるＤＬＬファイルを含むことがしばしばである。インストーラは、システムファイルを変更す

るその能力により、アプリケーションが設計通りに実行されるために必要な全てのファイルを有することになるのを確実にすることができる。しかし、このことは、他のアプリケーションが必要とする共用システムファイルに対してインストーラが不適切な変更を同じく加えることができるので、オペレーティングシステムをシステム不安定という重大な問題にも直面させる。例えば、より古いアプリケーションのインストーラは、システム上の既存のＤＬＬファイルを、より新しいアプリケーションとは一緒に働かないそのファイルのより古いバージョンで重ね書きする場合がある。ソフトウエア専門業者の中には、ＤＬＬファイルの他のアプリケーションと互換性のないいくつかの専売権付きバージョンで選ばれたＤＬＬファイルを重ね書きすることを試みるものもある。オペレーティングシステムが更に複雑化し、益々多くのアプリケーションが入手可能になるにつれて、アプリケーションのインストール又は更新の間に共用システムファイルが無効バージョンで重ね書きされる危険性が益々増大している。共用オペレーティングシステムファイルの不適切な変更に起因するシステムの不安定性は、最近ではユーザが体験する非常に重大な問題となっており、オペレーティングシステムを比較する際の重要な要素となっている。

【０００４】

（発明の開示）

上記の観点から、本発明は、共用システムファイルを保護するシステム及び方法を提供し、それは、アプリケーションのインストール又は更新中、又は、ユーザの行為により、アプリケーションによって共用されるＤＬＬファイルなどのシステムファイルが不適切に変更されないように保護をする。共用システムファイルを保護するために、オペレーティングシステムには、システムファイルの変更を監視するモニタリング構成要素が備えられる。保護されたシステムファイルが変更されている時、モニタリング構成要素は、オリジナルファイルのコピーを記憶し、その変更についてシステムファイル保護（ＳＦＰ）サービスに報告する。ＳＦＰサービスは、変更ファイルを検査して、そのファイルが有効か否かを判断する。変更ファイルが無効であれば、システムファイルは、モニタリング構成要素により記憶されたコピーを用いてそのオリジナルの内容に復元される。アプリ

ケーション・インストーラ又は更新パッケージによるシステムファイルの未許可の持ち込みは、そのシステムファイルがインストールされることを表すそのパッケージに関する有効な証明書を要求することにより同じく防止される。

本発明の更なる形態や利点は、添付図面の参照と共に進められる例証的な実施形態に関する以下の詳細な説明から明らかになるであろう。

添付請求項は、本発明の形態を詳細に列挙するが、その目的及び利点と共に本発明は、添付図面に関連して為される以下の詳細な説明によって最も良く理解することができる。

【０００５】

（発明を実施するための最良の形態）

同様な参照番号が同様な部材を示す添付図面を参照すると、本発明は、適切な計算環境に実装された状態で示されている。必ずしもそれに限定されないが、本発明は、パーソナルコンピュータによって実行される、プログラムモジュールなどのコンピュータ実行可能命令との一般的な関連において以下に記述される。一般にプログラムモジュールは、特定のタスクを実行するか、又は、特定の抽象的データタイプを実装する、ルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。更に、手持式装置、マルチプロセッサシステム、マイクロプロセッサ式又はプログラム可能な消費者向け電子機器、ネットワーク・パーソナルコンピュータ、ミニコンピュータ、及び、メインフレームコンピュータなどを含む、他のコンピュータシステム形態を用いて本発明を実施してもよいことを当業者は理解するであろう。本発明はまた、タスクが通信ネットワークを通じて接続された遠隔処理装置によって実行される分散型計算環境において実施してもよい。分散型計算環境においては、プログラムモジュールは、ローカル及び遠隔記憶装置の両方に置くことができる。

【０００６】

図１を参照すると、本発明を実装する例示的システムは、汎用計算装置を従来のパーソナルコンピュータ２０の形で含んでおり、この汎用計算装置は、処理ユニット２１、システムメモリ２２、及び、システムメモリを含む様々なシステム構成要素を処理ユニット２１に結合するシステムバス２３を含む。システムバス

２３は、メモリバス又はメモリ制御装置、周辺バス、及び、様々なバス構造のいずれかを用いるローカルバスを含む幾つかの種類のバス構造のいずれでもよい。

システムメモリは、読取り専用メモリ（ＲＯＭ）２４とランダムアクセスメモリ（ＲＡＭ）２５とを含む。起動時などにパーソナルコンピュータ２０内における素子間の情報転送を補助する基本ルーチンを包含する基本入出力システム（ＢＩＯＳ）２６は、ＲＯＭ２４に記憶される。パーソナルコンピュータ２０は、ハードディスク６０に対して読出し及び書込みを行うハードディスクドライブ２７、取外し可能磁気ディスク２９に対して読出し又は書込みを行う磁気ディスクドライブ２８、及び、コンパクト・ディスク・ＲＯＭや他の光学的手段などの取外し可能光学ディスク３１に対して読出し又は書込みを行う光学ディスクドライブ３０を更に含む。

【０００７】

ハードディスクドライブ２７、磁気ディスクドライブ２８、及び、光学ディスクドライブ３０は、各々、ハードディスクドライブインタフェース３２、磁気ディスクドライブインタフェース３３、及び、光学ディスクドライブインタフェース３４により、システムバス２３に接続されている。これらのドライブとそれらに付随するコンピュータ読取可能手段は、コンピュータ読取可能命令、データ構造、プログラムモジュール、及び、パーソナルコンピュータ２０のための他のデータの不揮発性記憶装置を準備する。本明細書で説明する例示的環境は、ハードディスク６０、取外し可能磁気ディスク２９、及び、取外し可能光学ディスク３１を採用するが、磁気カセット、フラッシュメモリカード、デジタルビデオディスク、ベルヌーイカートリッジ、ランダムアクセスメモリ、及び、読取り専用メモリなど、データを記憶できるコンピュータでアクセス可能な他の種類のコンピュータ読取可能手段を例示的作動環境で同じく使用してもよいことは当業者により理解されるであろう。

【０００８】

オペレーティングシステム３５、１つ又はそれ以上のアプリケーションプログラム３６、他のプログラムモジュール３７、及び、プログラムデータ３８を含むいくつかのプログラムモジュールは、ハードディスク６０、磁気ディスク２９、

光学ディスク３１、ＲＯＭ２４，又は、ＲＡＭ２５上に記憶してもよい。ユーザは、キーボード４０や指示装置４２などの入力装置を通じてパーソナルコンピュータ２０の中に指令及び情報を入力することができる。他の入力装置（図示しない）には、マイクロホン、操作棒、ゲームパッド、衛星用ディッシュ、及び、走査器などが含まれてもよい。これら及び他の入力装置は、システムバスに結合されたシリアルポートインタフェース４６を通じて処理ユニット２１に接続されることが多いが、パラレルポート、ゲームポート、又は、ユニバーサルシリアルバス（ＵＳＢ）などの他のインタフェースによって接続されてもよい。モニタ４７又は他の種類の表示装置は、ビデオアダプタ４８などのインタフェースを通じて同じくシステムバス２３に接続される。モニタに加えてパーソナルコンピュータは、一般的にスピーカやプリンタなどの図示しないが他の周辺出力装置を含む。

【０００９】

パーソナルコンピュータ２０は、遠隔コンピュータ４９などの１つ又はそれ以上の遠隔コンピュータへの論理結合を用いるネットワーク環境で作動してもよい。遠隔コンピュータ４９は、別のパーソナルコンピュータ、サーバ、ルータ、ネットワークパーソナルコンピュータ、ピア装置、又は、他の普通のネットワークノードであってもよく、図１にはただ記憶装置５０のみが示されているが、通常、パーソナルコンピュータ２０に関して上記で説明した構成品の多く又は全てを含む。図１に示された論理結合は、ローカルエリアネットワーク（ＬＡＮ）５１とワイドエリアネットワーク（ＷＡＮ）５２とを含む。そのようなネットワーク環境は、事務所、企業間コンピュータネットワーク、イントラネット、及び、インターネットにおいてありふれたものである。

【００１０】

ＬＡＮのネットワーク環境で使用される場合、パーソナルコンピュータ２０は、ネットワークインタフェース又はアダプタ５３を通じてローカルネットワーク５１に接続される。ＷＡＮのネットワーク環境で使用される場合、パーソナルコンピュータ２０は、一般的には、ＷＡＮ５２上の通信を確立するためにモデム５４又は他の手段を含む。内臓モデム又は外付けモデムであり得るモデム５４は、シリアルポートインタフェース４６を通じてシステムバス２３に接続される。ネ

ットワーク環境においては、パーソナルコンピュータ２０又はその一部分に対して書かれたプログラムモジュールは、遠隔記憶装置に記憶することができる。図示のネットワーク接続は例証的であり、コンピュータ間の通信リンクを確立する他の手段を使用してもよいことが理解されるであろう。

【００１１】

以下の記述において、特に断らない限り、本発明は、１つ又はそれ以上のコンピュータによって実行される作用か、又は、作動の記号的表示かに関連して説明される。従って、時には「コンピュータで実行された」として言及されるそのような作用又は作動は、データの構造化された形態を表す電気信号をコンピュータの処理ユニットが操作することを含むことが理解されるであろう。この操作は、データを変換するか、又は、当業者にはよく理解されている方法でコンピュータの作動を再構成又はそうでなければ変更するコンピュータのメモリシステムの各位置にデータを保持する。データが維持されるデータ構造は、データ書式により規定される特質を有するメモリの物理的位置である。しかし、本発明は上記の関連で記述されているが、当業者が理解するように、それは限定的であることを意味せず、以下に述べる様々な作用及び作動は、ハードウエアに実装されてもよい。

【００１２】

ここで図２を参照すると、本発明は、ＤＬＬファイルなどの共用システムファイルを不注意で無効バージョンにより重ね書きされたり、又は、他の方法で不適当に変更されることから保護する効果的な方法に関する。以下に説明する好ましい実施形態において、オペレーティングシステムは、マイクロソフト・コーポレーションのＷＩＮＤＯＷＳ（登録商標）オペレーティングシステムであってもよく、アプリケーションによって共用され、保護されるシステムファイルの一例として、ＤＬＬファイルが使用される。しかし、本発明によるシステムファイル保護は、共用システムファイルを有する他のオペレーティングシステムと共に使用されるほか、他の種類の共用システムファイルを保護するためにも使用できるということが理解されるであろう。

【００１３】

図２に示すように、オペレーティングシステム７０は、実行中に様々なシステム機能を提供するために呼び出されてアプリケーション７４に動的に接続することができる複数のダイナミックリンクライブラリ（ＤＬＬ）ファイル７２を有する。ＤＬＬファイルに関しては、高められた機能をもたらすため又はバグを取り除くために過去に何度も更新されていることは普通のことであるから、与えられたＤＬＬファイルの幾つかの異なるバージョンが存在する場合がある。ＤＬＬファイルの異なるバージョンを憶えておくために、図示の実施形態における各ＤＬＬファイルは、その名前によって識別されるだけでなく、付随するバージョン番号によっても識別される。

【００１４】

上記の通り、システム不安定性の１つの主要原因は、アプリケーションのインストレーション又は更新パッケージ６６のインストーラが現存の共用システムファイルを他のアプリケーションと共には実行できないバージョンで重ね書きすることを試みる場合があるということである。例えば、より古いアプリケーションは、より古いバージョンでＤＬＬファイルの重ね書きを試みる場合があり、又は、あるアプリケーションは、他のアプリケーションと適合しない専売権付きバージョンでＤＬＬファイルの重ね書きを試みる場合もある。アプリケーションのインストレーション又は更新は、共用システムファイルが不適切に重ね書きされたり、又は、他の方法で変造や破壊される筋書きの１つであるに過ぎないことが理解されるであろう。例えば、共用システムファイルは、ユーザ６８の行為により不適切に変更されたり、削除されたりすることもある。以下の記述の観点から明らかになるように、本発明によるシステムファイル保護は、そのようなユーザの行為に対しても、また同様に、保護されたシステムファイルを未許可に変更する他の原因に対しても同じく有効である。

【００１５】

本発明によれば、共用システムファイルの保護は、２つの関連する態様において実行される。第１に、すでにシステムに存在するシステムファイルは、無効なファイルで重ね書きされることから保護される。この目的のために、システムファイルの変更が監視される。保護されたシステムファイルが無効なファイルで重

ね書きされるか又は他の方法で不適切に変更されると、この無効な変更が検知されて取り消され、オリジナルファイルを復元する。第２に、アプリケーションのインストレーション又は更新中におけるシステムファイルの未許可の持ち込みは許可されず、システムに無効なシステムファイルが追加されるのを防ぐ。

【００１６】

第１の態様に戻ると、図示の実施形態において、未許可の変更からの現存システムファイルの保護は、ファイル変更モニタリング構成要素とシステムファイル保護（ＳＦＰ）サービス構成要素８０との協働によって達成される。図示の実施形態において仮想デバイスドライバ（Ｖｘｄ）８２として示されているモニタリング構成要素は、保護システムファイルの変更を監視し、この変更をＳＦＰサービス８０に告げる責任がある。これらが無効な変更であると判断された場合、ＳＦＰサービス８０は、この変更を取り消すことができる。図２に示すように、オペレーティングシステム７０のファイルシステムマネージャ８６とファイルシステムドライバ８８との間には、モニタリング構成要素（Ｖｘｄ）８２が挿入されている。Ｖｘｄ８２をこの位置に有することにより、システムメモリ９０に記憶されたファイルに対する作動のためのシステムファイルマネージャ８６からシステムファイルドライバ８８への全ての呼び出しは、Ｖｘｄを通過することになる。このようにして、Ｖｘｄ８２は、システムファイルのあらゆる変更を追跡することができる。ファイルの変更としては、ファイルを別のファイルで重ね書きすること、ファイルのいくつかのデータを変更すること、又は、ファイルを削除することに関わる場合がある。

【００１７】

Ｖｘｄ８２がファイルを変更する呼び出しを受け取った時、Ｖｘｄ８２は、そのファイルについて責任のあるファイルシステムドライバ８８に向けてその呼び出しを直ちには転送しない。その代わりに、Ｖｘｄは、最初に保護システムファイルのリスト９２を検査し、変更されるこのファイルが本実施形態においてはＤＬＬファイルを含む保護システムファイルのうちの１つであるか否かを調べる。そのファイルが保護システムファイルである場合、Ｖｘｄ８２は、最初にオリジナルファイルのコピーを作成し、変更が為されるのを許可する前に、このコピー

をシステムの一時的ディレクトリ９６に記憶する。次いで、Ｖｘｄ８２は、ＳＦＰサービス８０に対して保護ファイルが変更されたことを報告する。図示の実施形態においては、Ｖｘｄ８２とＳＦＰサービス８０との間の通信は、ＷＩＮＤＯＷＳ（登録商標）のメッセージによるものであり、ＳＦＰサービスは、メッセージループで実行されている。

【００１８】

一例として、図２に示すように、変更されるシステムファイルは、バージョン番号２を有する「ａｂｃ．ｄｌｌ」と名付けられたファイルであってもよい。このファイルをａｂｃ．ｄｌｌのバージョン１で重ね書きするという呼び出しを受け取った時、Ｖｘｄ８２は、保護ファイルのリスト９２を検査してこのファイルが保護されるべきであると判断する。次に、Ｖｘｄ８２は、ａｂｃ．ｄｌｌのｖ２（バージョン２）のコピーを一時的ディレクトリ９６に記憶する。システムメモリ９０のファイルａｂｃ．ｄｌｌのｖ２は、次に、ａｂｃ．ｄｌｌのｖ１（バージョン１）で置き換えられる。

【００１９】

ＳＦＰサービス８０は、Ｖｘｄ８２から保護システムファイルが変更されたとの報告を受け取ると、その変更が許されるか否かを検査する。オリジナルファイルが新しいファイルで重ね書きされる場合、ＳＦＰサービスは、新しいファイルが有効か否かを判断する。新しいファイルが無効である場合、ＳＦＰサービス８０は、Ｖｘｄ８２によって一時的ディレクトリに記憶されたオリジナルファイルのコピーでこの新しいファイルを置き換え、それによってその変更を取り消す。

【００２０】

いくつかの場合には、保護ファイルに対する意図された変更は直ちには実行されないで、後で実行すべく延期される。例えば、共用システムファイルが連続的に使用されており、それへの書き込み作動が実行できない場合には、ファイルシステムマネージャは、目標のシステムファイルを新しいファイルで重ね書きする書込命令１００をシステム起動ファイル９８に置くように決めることができる。システムが次回に起動されると、システム起動ファイルの書込命令が実行されることになり、変更が達成される。この筋書きの場合、新しいファイルが無効であ

るとＳＦＰサービス８０が判断した場合、ＳＦＰサービス８０は、単に書込命令１００をシステム起動ファイルから除去するだけであり、これによって無効な変更が起こるのを防止する。

【００２１】

これと関連する筋書きにおいて、ＳＦＰサービス８０が新しいファイルは無効であると判断したが、アプリケーションによるこのシステムファイルの連続使用がＳＦＰサービス８０によるオリジナルファイルの復元を制限する時、オリジナルシステムファイルの無効なバージョンによる重ね書きが既に起こっている場合がある。この場合には、Ｖｘｄ８２により保存されたオリジナルファイルのコピーで変更されたシステムファイルを重ね書きするために、ＳＦＰサービス８０は、書込命令１０２をシステム起動ファイル９８に置くように決めることができる。すなわち、次回のシステム起動中に、システムファイルはそのオリジナルの形に復元されることになる。

【００２２】

ある実施形態においては、Ｖｘｄ８２により検査される保護システムファイルのリスト９２は、拡張可能なマークアップ言語（ＸＭＬ）書式でファイルに含まれる。説明の便宜上、図３は、そのようなＸＭＬファイルの単純化された例を示している。この例において、ＸＭＬファイル１０６は、他のシステム管理目的のためにファイルを識別するためにも使用される。保護される共用システムファイルは、段落１０８において「ＳＥＰ」タグを用いて識別される。図を単純化するために、図３に示すＸＭＬファイル１０６の「ＳＦＰ」段落は、２つのエントリのみを含む。しかし、実際の実行に際しては、保護されたシステムディレクトリやファイルを識別するために、この段落には多くのエントリがあってもよいことが理解されるであろう。この実施形態においては、この「ＳＦＰ」段落の各ステートメントは、保護されるシステムファイル（それが入っているディレクトリを含む）を識別する。ＸＭＬファイルは、オペレーティングシステムを備えており、ファイルをリストに加えたり、又は、リストから除去する必要がある時には、更新パッケージを用いて更新することができる。システムファイルが書込演算のために開かれている時、Ｖｘｄ８２は、ＸＭＬファイルを検査し、システムファ

イルがＸＭＬファイルの「ＳＦＰ」段落に現れているか否かを調べる。もし現れていれば、システムファイルは保護されることになり、Ｖｘｄは、そのシステムファイルがいかなる変更を受けるよりも前にそのコピーを作成する。

【００２３】

変更システムファイルが有効か否かをＳＦＰサービス８０が判断できるようにするために、ＳＦＰサービスは、システム上にインストールされた共用システムファイルを識別するシステムファイル保護（ＳＦＰ）データベース１１０を保持する。説明の便宜上、図４にＳＦＰデータベース１１０の例を表の形式で示す。システムファイルの持ち込み制御と関連して一層詳細に後述するように、アプリケーション・インストーラ又は更新パッケージによって加えられるシステムファイルは、オペレーティングシステムに呈示される１つ又はそれ以上のカタログで識別されるのが好ましい。図４に示すように、ＳＦＰデータベース１１０の各エントリは、保護されたＤＬＬファイルの名称とそのファイルが提示されたカタログのほか、そのカタログで特定されたそのファイルのバージョン番号を記憶する。ある与えられたファイル名が多くのカタログに列挙されている場合、同一ファイル名を有する多くのエントリが存在してもよい。ただし、同一ファイル名を有するエントリの各々は、異なるバージョン番号及び／又はそれに付随するカタログ名を有することになるであろう。例えば、図４に示す例においては、Ｗｉｎｓｏｃｋ．ｄｌｌに対して２つのエントリが存在しており、それらは、各々、カタログのＭｉｌｌ．ｃａｔとＭｉｌｌＳＰ１．ｃａｔとに付随し、バージョン番号の６．０と７．０とを有する。

【００２４】

好ましい実施形態の態様によれば、保護システムファイルは、そのファイル名とバージョン番号とによってのみならず、ハッシュ値によっても識別される。ある与えられたファイルのハッシュ値は、ハッシュ関数をファイルの内容に適用することによって作り出される。ハッシュ関数とは、ファイルにおける１つのビットの変更さえも異なるハッシュ値をもたらす可能性が高くなるといったようなものである。同時に、ハッシュ値から逆にファイルの内容を引き出すことはできない。後述するように、保護システムファイルをそのハッシュ値で識別することは

、そのファイル名とバージョン番号とが同じままであるにもかかわらず、その内容が変更されたか否かの判断を可能にする。好ましい実施形態においては、保護システムファイルのハッシュ値は、そのファイルをシステム上にインストールするために使用された対応するカタログに記憶され、カタログは、システムのカタログ記憶装置１４０（図５）に保持される。

【００２５】

保護システムファイルが変更されたというＶｘｄ８２からのメッセージをＳＦＰサービス８０が受け取った時、ＳＦＰサービスは、ＳＦＰデータベース１１０に対して、変更されたものと同じファイル名を有するデータベース内の全てのエントリを問い合わせる。次に、ＳＦＰサービスは、データベースからの情報に基づいて、その「新しいファイル」が有効か否かを判断する。新しいファイルは、（１）新しいファイルがＳＦＰデータベースのそのファイルに対するエントリの最高バージョン番号と同じバージョン番号を有し、（２）新しいファイルがそのバージョン番号に対する正しいハッシュ値を有する場合、それは有効と見なされる。この２番目の比較に関して、ＳＦＰサービス８０は、ＳＦＰデータベースエントリの最高バージョン番号を読み取ってこれに付随するカタログを識別し、そのバージョンに対するハッシュ値を得るためにカタログ記憶装置１４０のそのカタログを読み出す。新しいファイルが正しいハッシュ値を持つことを必要とすることは、オリジナルファイルが同じファイル名と正しいバージョン番号とを有するが変更されて無効な内容を有するファイルで重ね書きされる危険性を防止する。

【００２６】

ここで、本発明によるファイル保護の第２の態様に戻ると、システムファイルの持ち込みは綿密に監視され、それらが適正な許可の表示を伴っている場合にのみシステムに加えることが許可される。好ましい実施形態においては、システムファイルの持ち込みは、アプリケーション・インストレーション又はアプリケーション更新パッケージのいずれかによって行うことができる。いずれの場合にも、システムに置かれるシステムファイルは、カタログに提示される。カタログで識別されたシステムファイルをインストールする演算は、アプリケーションをイ

ンストールする場合と更新パッケージをインストールする場合の両方で同じであるから、以下では更新パッケージをインストールする場合についてのみ記述される。この観点から言えば、アプリケーション・インストレーション・パッケージは更新パッケージの一種であると見なしてもよいことが理解されるであろう。

【００２７】

図５は、説明のためにカタログ１２０の例を示す。カタログは多重エントリを有してもよく、各エントリは、システムに加えられるシステムファイルを識別する。エントリは、例えば、ファイル名、そのファイルのハッシュ値、及び、ファイルのバージョン番号を準備する。エントリは、ファイルに関する他のデータを同じく含んでもよい。図示の実施形態においては、カタログは、システムにインストールされる更新パッケージ１２２の一部である。

【００２８】

無効なファイルがシステムに持ち込まれて共用システムファイルを重ね書きするために使用されるのを防ぐために、更新パッケージ１２２には、そのカタログ及び付随するファイル１２６が受け入れられることになる前に適正な許可を示すことが要求される。好ましい実施形態においては、この許可検査は、更新パッケージ１２２と共に含まれる証明書１２８によって行なわれる。この証明書１２８は、パッケージの真正性と完全性とを保証する良く知られた証明書型認証技術に従って適切な証明書機関１３２によって発行することができる。証明書を発行する証明書機関１３２は、例えば、オペレーティングシステムの製造会社であってもよいし、又は、正しく作られたインストレーション又は更新パッケージを証明する責任を委託されたいかなる他の関係者であってもよい。保護システムファイルのいかなるインストレーションも有効な証明書を伴うことが必要であることにより、その証明書を発行する機関１３２は、パッケージに呈示された全てのシステムファイルが有効であることを検査することができる。

【００２９】

一般に、更新パッケージ１２２は、インストーラ１３６、１つ又はそれ以上のカタログ１２０、及び、システムに加えられる全てのシステムファイル及びアプリケーションファイル１２６を包含する圧縮キャビネット（ＣＡＢ）ファイル１

２４の形態を有する。オペレーティングシステムがＣＡＢファイルを用いて提示された時、オペレーティングシステムは、最初に、パッケージに含まれている証明書１２８が適切な機関によって発行されたか否かを検査する。適切な機関によって発行されている場合は、ファイルの完全性、すなわちファイルが変更されたことがないことを証明するために証明書が用いられる。証明書を認証した後、ＣＡＢファイル内に圧縮されたファイルが取り出される。パッケージ内のインストーラ１３６は、上記の通り、次にカタログとカタログに列挙されたファイルとをインストールすることを許される。

【００３０】

カタログ１２０で識別されたシステムファイルをインストールするために、更新パッケージ１２２のシステム構成要素インストーラ１３６は、オペレーティングシステムのカタログ・アプリケーションプログラミングインタフェース（ＡＰＩ）１３８を呼び出す。カタログＡＰＩ１３８は、インストールカタログ（ＩｎｓｔａｌｌＣａｔａｌｏｇ）機能とアンインストールカタログ（ＵｎｉｎｓｔａｌｌＣａｔａｌｏｇ）機能とを呈示する。カタログ１２０で識別されたシステムファイルをインストールするために、インストーラ１３６は、インストールカタログ機能を呼び出してカタログを提示する。これに呼応して、ＳＦＰサービス８０は、カタログ１２０のエントリを列挙してこれらを上記の通りＳＦＰデータベースに加え、システムファイルをそれらの適正ディレクトリにコピーする。カタログ１２０は、カタログ記憶装置１４０にも加えられる。その後、ＳＦＰデータベース１１０がいくらか変造された場合、システムにインストールされた保護システムファイルを特定するためにカタログ記憶装置１４０の全てのカタログを列挙することにより、ＳＦＰデータベースを再構築することができる。

更新パッケージのインストーラがカタログの除去を欲する時、インストーラは、カタログＡＰＩ１３８のアンインストールカタログ機能を呼び出す。このアンインストール要求に応答して、ＳＦＰサービス８０は、ＳＦＰデータベース１１０に対してデータベースにあるその与えられたカタログに付随する全てのエントリについて問い合わせ、それらのエントリをデータベースから除去する。

【００３１】

本発明の原理を適用し得る多くの可能な実施形態の観点において、図面の各図に関連して本明細書で記述した実施形態は単に例証的であることを意味しており、本発明の範囲を限定するように解釈してはならないことを理解されたい。例えば、ソフトウエアの形で示され説明された実施形態の要素をハードウエアに実装してもよいしその逆もまた可能であり、あるいは、説明された実施形態が本発明の精神から逸脱することなく構成や細部を変更できることを当業者は理解するであろう。従って、本明細書で記述された本発明は、そのような全ての実施形態が添付請求項及びその同等形態の範囲に該当するように意図されている。

【図面の簡単な説明】

【図１】

本発明が適用される例示的コンピュータシステムを一般的に示すブロック図である。

【図２】

共用システムファイルを保護する本発明による構成要素を有するオペレーティングシステムの実施形態を示す概略図である。

【図３】

保護されるシステムファイルを識別する図２の実施形態で使用される例示的ＸＭＬファイルを示す図である。

【図４】

保護システムファイルに関する情報を提供するシステムファイル保護（ＳＦＰ）データベースにおけるデータ構造の概略図である。

【図５】

有効な証明書の提示に基づくインストレーション／更新パッケージにより与えられるシステムファイルの制御された持ち込みを示す概略図である。

【図１】

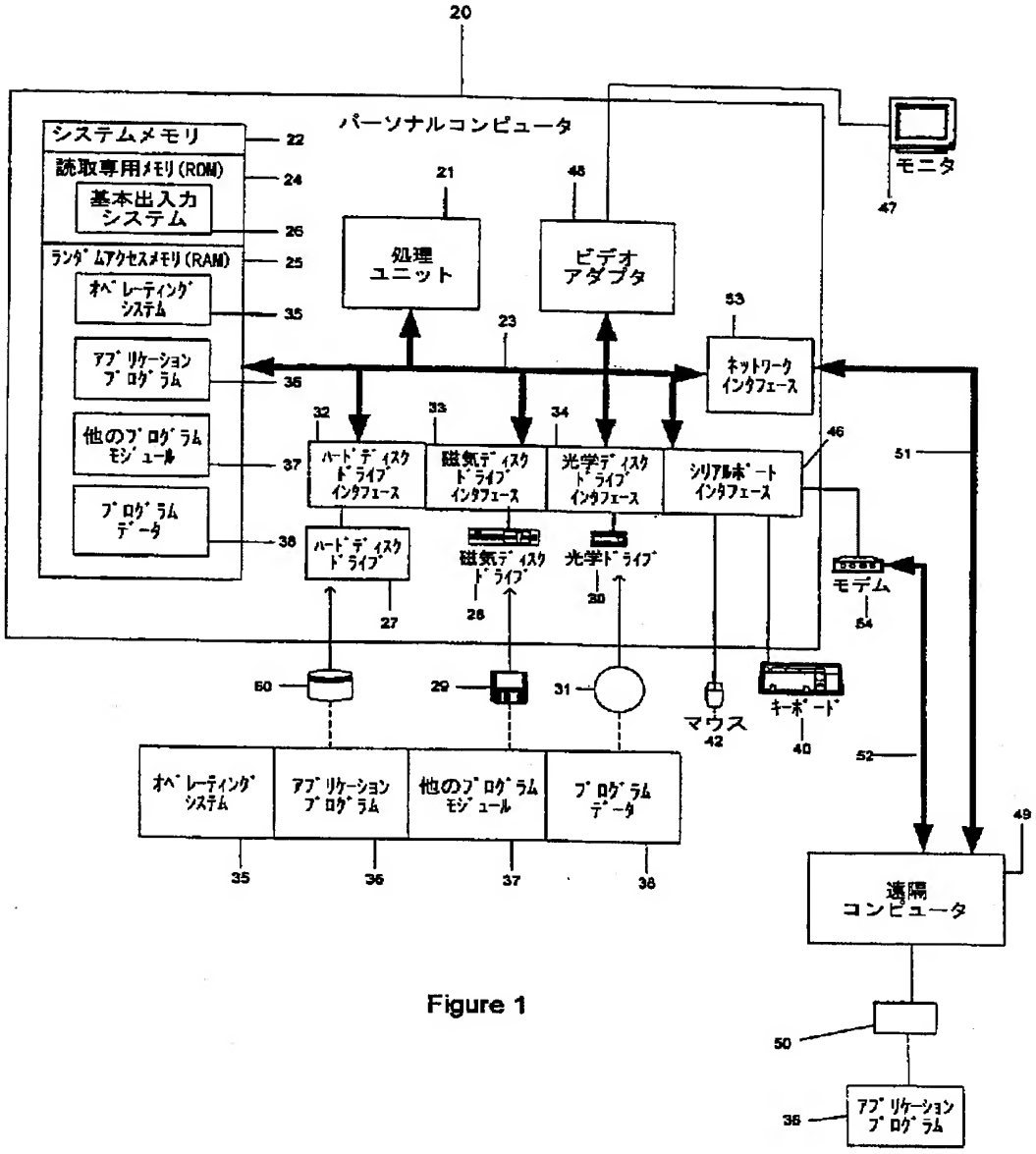

20
パーソナルコンピュータ
システムメモリ
22
読取専用メモリ(ROM)
24
基本出入力システム
26
ランダムアクセスメモリ(RAM)
25
オペレーティングシステム
35
アプリケーションプログラム
36
他のプログラムモジュール
37
プログラムデータ
38
処理ユニット
21
ビデオアダプタ
48
モニタ
47
23
ネットワークインタフェース
53
32
33
34
ハードディスクドライブインタフェース
磁気ディスクドライブインタフェース
光学ディスクドライブインタフェース
シリアルポートインタフェース
46
51
ハードディスクドライブ
27
磁気ディスクドライブ
28
光学ドライブ
30
モデム
54
60
29
31
マウス
42
キーボード
40
52
オペレーティングシステム
アプリケーションプログラム
他のプログラムモジュール
プログラムデータ
35
36
37
38
遠隔コンピュータ
49
50
アプリケーションプログラム
36

Figure 1

【図２】

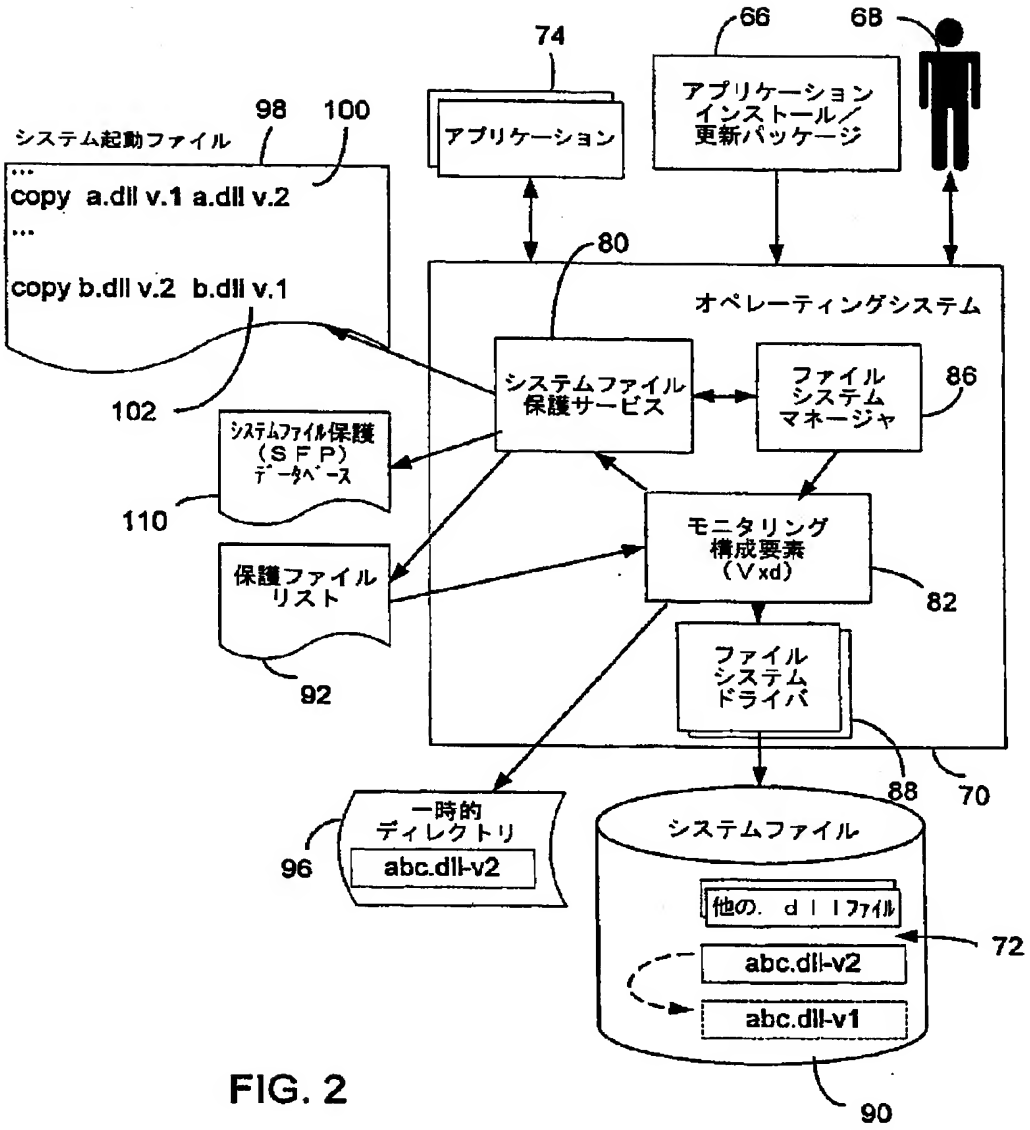

74
66
68
アプリケーション
アプリケーション
インストール／
更新パッケージ
98
100
システム起動ファイル
...
copy a.dll v.1 a.dll v.2
...
copy b.dll v.2 b.dll v.1
80
オペレーティングシステム
システムファイル
保護サービス
ファイル
システム
マネージャ
86
102
システムファイル保護
（ＳＦＰ）
データベース
110
モニタリング
構成要素
（Ｖxd）
82
保護ファイル
リスト
92
ファイル
システム
ドライバ
88
70
一時的
ディレクトリ
96
abc.dll-v2
システムファイル
他の．ｄｌｌファイル
72
abc.dll-v2
abc.dll-v1
90

FIG. 2

【図３】

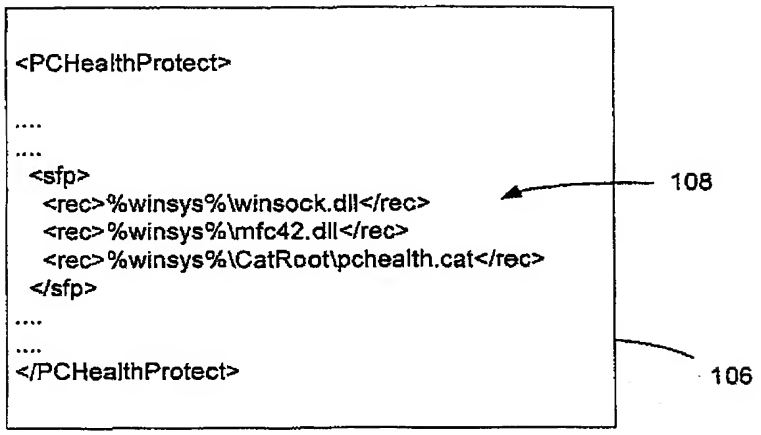
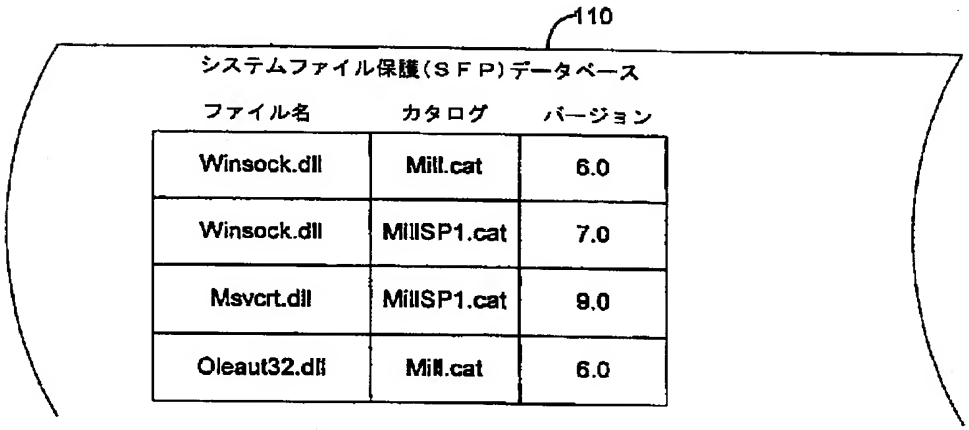


FIG. 3

【図４】

FIG. 4



【図５】

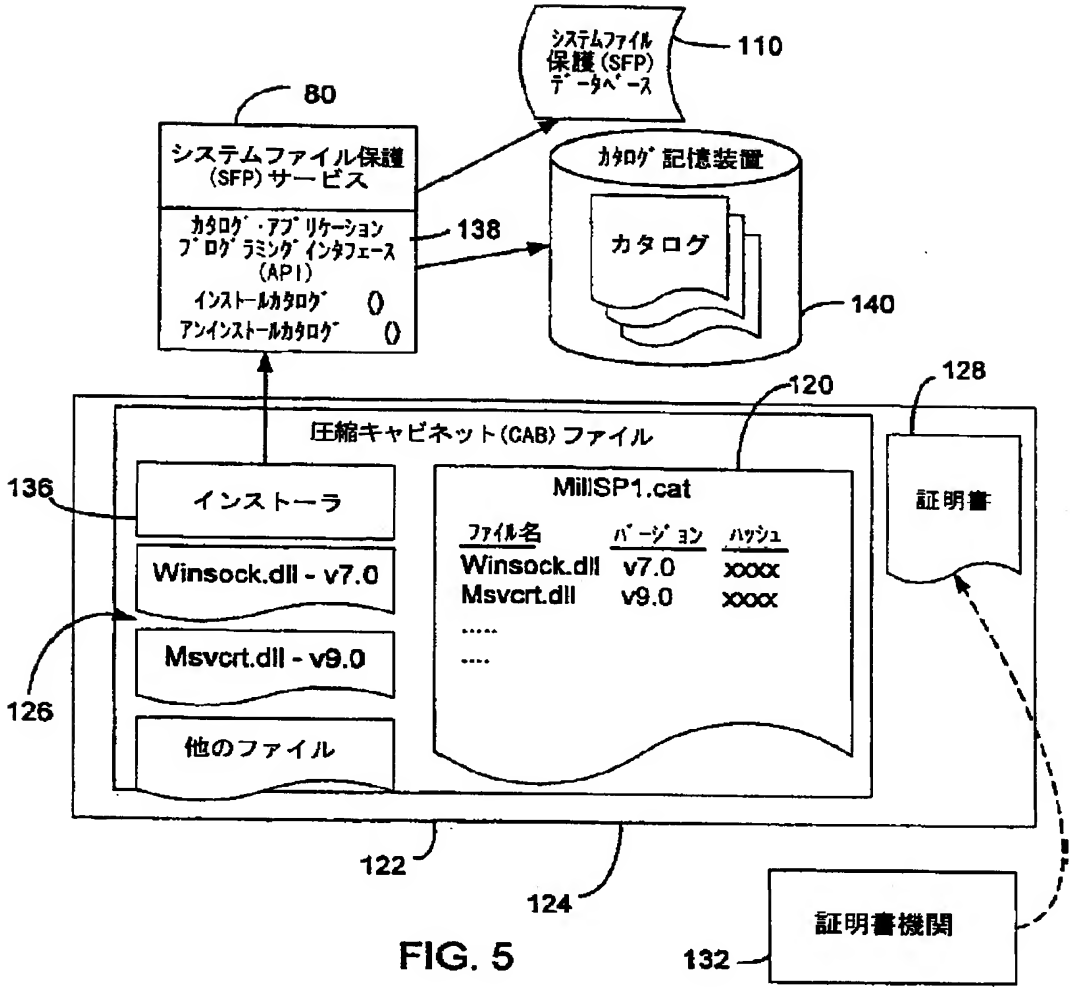

システムファイル
保護(SFP)
データベース
110
80
システムファイル保護
(SFP)サービス
カタログ・アプリケーション
プログラミング・インタフェース
(API)
インストールカタログ ()
アンインストールカタログ ()
138
カタログ記憶装置
カタログ
140
120
128
圧縮キャビネット(CAB)ファイル
136
インストーラ
Winsock.dll - v7.0
Msvcrt.dll - v9.0
他のファイル
126
MillSP1.cat
ファイル名 バージョン ハッシュ
Winsock.dll v7.0 xxxx
Msvcrt.dll v9.0 xxxx
.....
....
証明書
122
124
証明書機関
132

FIG. 5

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/US 00/18324

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F11/14 G06F9/44

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"SAFE INSTALLATION OF OBJECT-ORIENTED CLASS LIBRARIES COMMON TO MULTIPLE SOFTWARE PRODUCTS" IBM TECHNICAL DISCLOSURE BULLETIN,US,IBM CORP. NEW YORK, vol. 37, no. 2B, 1 February 1994 (1994-02-01), pages 407-409, XP000433893 ISSN: 0018-8689 * the whole document *	1-3,9, 11-13, 15,22
A	US 5 715 462 A (BRYEN MARK D ET AL) 3 February 1998 (1998-02-03) column 3, line 43 -column 6, line 9; claims 1,2	13-17

-/--

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 December 2000	11/12/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Fransen, L

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr nal Application No
PCT/US 00/18324

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	COLLINSON: "Putting old software back together again" EXE , vol. 13, no. 6, November 1998 (1998-11), pages 45-48, XP000965369 UK page 45, right-hand column -page 46, left-hand column	1-4

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

...formation on patent family members

Inter nal Application No
PCT/US 00/18324

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5715462 A	03-02-1998	JP 7281934 A	27-10-1995
		CN 1127043 A	17-07-1996
		DE 19580589 T	27-06-1996
		GB 2294568 A,B	01-05-1996
		WO 9527941 A	19-10-1995
		KR 176272 B	15-05-1999

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(81)指定国　EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW

(72)発明者　トーマス　アニル　フランシス
アメリカ合衆国　ワシントン州　98052
レッドモンド　ノースイースト　フィフティーフィフス　ストリート　18470

(72)発明者　ジャマル　ハウルーン　エム　エイ
アメリカ合衆国　ワシントン州　92846
レッドモンド　ワンハンドレッドアンドフィフティーセカンド　アヴェニュー　ノースイースト　6321

(72)発明者　クリシュナスワミ　ブリジェッシュ　エス
アメリカ合衆国　ワシントン州　98007
ベルヴュー　ノースイースト　サーティーンス　プレイス　#1908　15400

Fターム(参考)　5B076 FC06
5B082 DC05 DE07 FA16 GA14